

Handleiding: Aantonen van gelijkwaardigheid aan ISO 27001 bij aanbestedingen

Deze handleiding helpt inschrijvers die (nog) niet beschikken over een ISO 27001-certificaat, maar wel aantoonbaar voldoen aan gelijkwaardige informatiebeveiligingsmaatregelen. Het doel is om op een gestructureerde manier aan te tonen dat uw organisatie voldoet aan de aanbestedingseis 'ISO 27001 of vergelijkbaar', conform artikel 2.96 lid 2 van de Aanbestedingswet 2012.

1. Wettelijke basis

Artikel 2.96 lid 2 van de Aanbestedingswet 2012 bepaalt dat een aanbestedende dienst ook andere bewijzen inzake gelijkwaardige maatregelen moet aanvaarden wanneer de ondernemer het certificaat niet tijdig kon verwerven om redenen die hem niet aangerekend kunnen worden. Ook zonder formeel certificaat kan dus worden aangetoond dat uw informatiebeveiligingsmanagementsysteem (ISMS) gelijkwaardig functioneert aan de ISO 27001-norm.

2. Wanneer te gebruiken

Gebruik deze handleiding wanneer de aanbesteding vraagt om 'ISO 27001 of vergelijkbaar' en uw organisatie:

- (nog) geen ISO 27001-certificaat heeft, maar wel een ISMS volgens dezelfde principes;
- zich in het certificeringstraject bevindt;
- of werkt met een andere norm (zoals NEN 7510, TISAX of SOC 2) die inhoudelijk overeenkomt.

3. Stappenplan voor het aantonen van gelijkwaardigheid

Stap 1 – Inventariseer uw maatregelen: breng beleid, procedures, audits en risicoanalyses in kaart.

Stap 2 – Gebruik de Gelijkwaardigheidsmatrix ISO 27001 (Excel-sjabloon) en vul de kolommen in met uw maatregelen en bewijs.

Stap 3 – Verzamel bewijsstukken (beleid, auditrapporten, risicoanalyses, opleidingsplannen, externe beoordelingen).

Stap 4 – Voeg een managementverklaring toe waarin u verklaart dat uw ISMS voldoet aan de ISO 27001-principes.

Stap 5 – Controleer volledigheid: zorg dat alle onderdelen van ISO 27001 zijn afgedekt.

Stap 6 – Dien de documentatie in samen met uw inschrijving.

4. Tips voor een overtuigende onderbouwing

- Toon resultaatgelijkheid aan: uw maatregelen moeten hetzelfde beveiligingsniveau bieden.
- Wees concreet over verantwoordelijkheden, evaluaties en audits.
- Overweeg een onafhankelijke beoordeling door een externe securityconsultant.
- Houd uw bewijsstukken overzichtelijk en duidelijk gelabeld.

5. Voorbeeldstructuur van de inzending

Bijlage_ISO27001_of_vergelijkbaar/

- 1. Managementverklaring_ISMS.pdf
- 2. Gelijkwaardigheidsmatrix_ISO27001.xlsx
- 3. Beleid_Informatiebeveiliging.pdf
- 4. Risicoanalyse_ISMS_2025.pdf

- └─ 5. Auditrapport_Externe_Toetsing.pdf
- └─ 6. Planning_Certificering_ISO27001.pdf

6. Samenvatting

Met deze handleiding en de bijgevoegde matrix kunnen inschrijvers aantonen dat hun organisatie functioneel gelijkwaardig is aan ISO 27001. Zo kan de aanbestedende dienst een eerlijke beoordeling uitvoeren, ook wanneer formele certificering nog niet is afgerond.